MASTER TERMS DIRECT PURCHASING

Mercedes-Benz U.S. International, Inc.
Mercedes-Benz Vans, LLC
Mercedes-Benz ExTra LLC

DATA PROTECTION AND INFORMATION SECURITY REQUIREMENTS

Revision History

Revision Level	Change Date
1.0	1/3/2023

IMPORTANT: *Check with Buyer for any late-breaking changes to these directives.*

Mercedes-Benz
U.S. International, Inc.

Owner: Legal
Created: January 2023
Location: g:/legal/ims/controlled/masterterms/

Data Protection and Information Security Requirements

These **Data Protection and Information Security Requirements** (the "**Requirements**") supplement the Master Terms Direct Purchasing (the "**Agreement**") to which it is attached. All capitalized terms used herein shall have the meanings ascribed to them in these Requirements, or, if not so ascribed, as set forth in the Agreement.

1. Definitions.

1.1 **Industry Standards** means those standards applicable to the Supplier or Buyer, and the automotive industry.

1.2 **Buyer Data** means any commercially sensitive information about Buyer and all personal information protected under any Privacy and Security Laws that is provided to or accessible by Supplier as a result of the Agreement and/or these Requirements and any Confidential Information as defined in the Agreement. Buyer Data shall include, without limitation, all individual records or compilations that include transaction histories, transactional information, designs/drawings, product-level data, technical specifications, transaction channels, consumer marketing preference data, Buyer's employee compensation information, cost information, pricing information, consumer marketing preference data, lead generation sources or other sales related data, information regarding mergers, acquisitions or other transactions, or similar information. Further, Buyer Data shall include, without limitation, all information that: (i) identifies or can be used to identify an individual (including, without limitation, names, signatures, addresses, telephone numbers, e-mail addresses, vehicle identification number and other unique identifiers); or (ii) can be used to authenticate an individual (including, without limitation, employee identification numbers, government-issued identification numbers (including social security number, driver's license number or state-issued identified number), passwords or PINs, financial account number, credit card number, debit card number, credit report information, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account, credit report information, biometric or health data, answers to security questions and other personal identifiers); or (iii) any data regulated as personal information or personal data by Privacy and Security Laws. Buyer Data shall also include information regarding Buyer's information security program or infrastructure, including, without limitation, Buyer Systems.

1.3 **Buyer Information Security Contact** means an individual working for Buyer and assigned by Buyer to act as the security liaison between Buyer and Supplier with respect to information, data and infrastructure security, including (i) overseeing compliance with these Requirements, (ii) receiving notice of Security Breaches from Supplier or its permitted subcontractors, and (iii) coordinating Security Breach incident response and remedial action.

1.4 **Buyer Systems** means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, licensed or leased by Buyer, or operated by a third party on behalf of Buyer, which: (a) connects to or otherwise interacts with Supplier Systems; or (b) is enabled or intended to access or interact with Buyer Data Processed as part of the Services or in connection with the Agreement.

1.5 **Privacy and Security Laws** means all international, local country-specific, European, and US State and Federal laws, standards, guidelines, policies, regulations, and procedures, as amended, applicable to Supplier or Buyer pertaining to the security, confidentiality or privacy of the Buyer Data, including, without limitation, the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 113 Stat. 1338) and its implementing regulations, the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, the Alabama Data Breach Notification Law, and the General Data Protection Regulation (2016/679).

1.6 **Process** means to perform any operation or set of operations on Buyer Data, including, without

limitation, to: (a) create, collect, receive, input, upload, download, record, reproduce, store, host, organize, combine, log, catalog, cross-reference, manage, maintain, copy, adapt, alter, translate, or make other improvements or derivative works; (b) analyze, output, consult, use, disseminate, transmit, submit, post, transfer, disclose, or otherwise provide or make available; or (c) block, erase, delete, or destroy.

1.7 **Security** means Supplier's technological, physical, administrative, organizational and procedural safeguards, including, without limitation, policies, procedures, guidelines, practices, standards, controls, hardware, software, firmware, and physical security measures, the function or purpose of which is, in whole or part: (a) to protect the confidentiality, integrity or availability of Buyer Data, Buyer Systems and Supplier Systems; (b) to prevent the unauthorized use of or unauthorized access to Buyer Data, Buyer Systems and Supplier Systems; and/or (c) to prevent a breach or malicious infection of Buyer Data, Buyer Systems and Supplier Systems.

1.8 **Security Breach** means any actual or reasonably suspected: (a) unauthorized use of, or unauthorized access to Supplier Systems; (b) inability to access Buyer Data or Supplier Systems due to a malicious use, attack or exploit of such Buyer Data or Supplier Systems; (c) unauthorized access to, theft of or loss of Buyer Data; (d) unauthorized use of Buyer Data for purposes of actual or reasonably suspected theft, fraud or identity theft; (e) unauthorized disclosure of Buyer Data; (f) breach of, transmission of or infiltration of malicious code into, Buyer Systems arising from, in whole or part, an act, error, or omission by Supplier; of (g) receipt of a complaint in relation to the privacy practices of Supplier or a breach or alleged breach of this Agreement relating to such privacy practices.

1.9 **Security Coordinator** means an individual working for Supplier assigned by Supplier to act as its Security Coordinator, who will be the security liaison between Buyer and Supplier and (i) oversee compliance with these Requirements, (ii) receive notice of Security Breaches within the Supplier's organization, (iii) coordinate Security Breach incident response and remedial action, and (iv) provide notice, reporting and work within Supplier to undertake other actions and duties as set forth in these Requirements.

1.10 **Secure Development Practices** refers to the utilization of state of the art methods or processes to ensure that software is free of vulnerabilities at any time during the software life cycle. Secure Development Practices include, without limitation, observance of the OWASP framework and SANS Top 25 guidelines.

1.11 **Security Framework** refers to the ISO 27001 family of standards for Information Security Management Systems, the NIST Framework for improving Critical Infrastructure Cybersecurity, the Cloud Security Alliance Security Guidance, or any other security framework approved in writing by Buyer.

1.12 **Security Incident** means the successful or attempted exploitation of an existing vulnerability detrimental to the confidentiality, integrity, operability or availability of Buyer Data, Buyer Systems, or Supplier Systems.

1.13 **Services** means the service(s) that Supplier provides to Buyer under the terms of the Agreement or any applicable SOW thereunder.

1.14 **Supplier Systems** means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, leased or controlled by Supplier or operated by a third party on behalf of Supplier that Processes Buyer Data or is connected to any computer, computer network, computer application, storage device, mobile computing device or software owned, licensed or leased by Buyer.

2. Data Processing.

2.1 Only as Necessary. Supplier shall only Process Buyer Data to the extent necessary to provide the Services to Buyer or as otherwise expressly permitted in the Agreement, the applicable SOW, or other written instructions from Buyer, and for no other purpose.

2.2 Controls and Confidentiality. Supplier shall hold all Buyer Data in confidence. Supplier shall impose controls on (i) access to and viewing of Buyer Data, (ii) the copying of Buyer Data and (iii) the printing or other duplication of Buyer Data, and (iv) the distribution of Buyer Data. Supplier shall not under any circumstances sell or otherwise exchange for value, the Buyer Data.

2.3 Continuous Buyer Access. Except as explicitly provided in the Agreement, Supplier shall provide Buyer with unfettered, uninterrupted, and constant access to Buyer Data, and shall delete, correct, or block any Processing of such data, or allow Buyer to do the same, upon Buyer's written request.

2.4 Report Locations of Data. Upon request, Supplier shall provide to the Buyer Information Security Contact a list of each and every physical location at which either Supplier or Supplier's subcontractor(s) will Process Buyer Data. Supplier will Process the Buyer Data only in the locations / jurisdictions approved in writing by the Buyer.

2.5 List of Subcontractors. Supplier shall provide to Buyer a complete list of subcontractors who will Process Buyer Data in furtherance of Supplier's provision of Services to Buyer at the outset of the Agreement and shall update the list as necessary, provided however, that Supplier shall not engage a subcontractor to Process Buyer Data except as explicitly set forth in the Agreement or an SOW.

2.6 Reasonable Requests. Supplier shall comply with any reasonable request made by Buyer in order to respond to requests from authorities, data subjects, customers, or others to provide information (including details of the Services provided by Supplier) related to Supplier's Processing of Buyer Data.

2.7 Data Subject Requests. Supplier shall promptly notify Buyer if it receives any request from a data subject asserting rights under Privacy and Security Laws with respect to their personal data. Supplier will not respond to any such request except on the written instructions (including email) of Buyer. Supplier will provide Buyer with reasonable assistance in its efforts to fulfill its obligations to respond to such requests, including by providing access to or information about, deleting or modifying the relevant personal data, in each case, to the extent required under and in accordance with Privacy and Security Laws. If Supplier is unable to provide any such assistance for reasons permitted under Privacy and Security Laws, Supplier shall promptly notify Buyer of such fact and shall provide such assistance promptly after the reasons for not doing so have expired.

3. Information Security.

3.1 System Security. Supplier is responsible for the Security of Supplier's Systems and Buyer Data. Supplier shall, consistent with Industry Standards and its Security obligations under these Requirements, (i) collect and record information and (ii) maintain logs, planning documents, audit trails, records and reports concerning (a) its Security, (b) its compliance with these Requirements, Privacy and Security Laws and Security Breaches, (c) its storage, processing and transmission of Buyer Data and (d) the accessing and use of Supplier Systems.

3.2 Safeguards Generally. Supplier shall implement administrative, physical, and technical safeguards to protect Buyer Data that are no less rigorous than accepted Industry Standards, specifically: the International Organization for Standardization's latest version of ISO/IEC 27001, any other applicable Industry Standards for information security, and any Buyer standards provided to Supplier. Supplier shall ensure that all such safeguards, including safeguards related to the manner in which Buyer Data is Processed, comply with applicable Privacy and Security Laws and the terms and conditions of these Requirements. In the event of any conflict between (i) Supplier's obligation to employ and maintain reasonable, appropriate and adequate Security set forth herein, (ii) Supplier's obligation to meet Industry Standards for Security set forth herein, and (iii) Supplier's obligation to align with the ISO 27001 security standard or any other security-related obligation in this Agreement (including these Requirements), Supplier shall comply with the obligation that provides the most protective and rigorous Security.

3.3 Minimum Safeguards. At a minimum, Supplier's safeguards for the protection of Buyer Data shall include: (i) limiting access of Buyer Data to authorized employees; (ii) securing business facilities, data

centers, paper files, servers, back-up systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, device application, database and platform security; (iv) securing information. transmission, storage and disposal; (v) implementing authentication and access controls within media, applications, operating systems and equipment; (vi) use of multi-factor authentication when and where appropriate (vii) encrypting Buyer Data stored on any mobile device or media; (viii) encrypting Buyer Data that will be transmitted; (ix) strictly segregating Buyer Data from information of Supplier or its other customers so that Buyer Data is not commingled with any other types of information; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; (xi) providing appropriate privacy and information security training to Supplier's employees, contractors and other personnel; (xii) record maintenance, including, without limitation, incident and compliance recordkeeping with the Security Framework; (xiii) Secure Development Practices with regard to applications that Process Buyer Data; and (xiv) incident response, vulnerability mitigation, and vendor management programs.

3.4 Remote Access. Remote access to Buyer Data and/or Buyer Systems is only allowed upon prior written approval by Buyer, and must occur through access points approved buy Buyer. Supplier Systems used for such remote access must be protected according to these Requirements.

3.5 Supplier Devices. Supplier shall ensure only Supplier-owned, managed, or leased end-user devices are used by Supplier to Process Buyer Data and shall notify Buyer of any lost, stolen, or otherwise compromised device that was used to Process Buyer Data in the manner required for Breach Notifications pursuant to Section 4 of these Requirements.

3.6 Subcontractor Devices. Supplier shall ensure that subcontractors shall only use subcontractor-owned, managed, or leased end-user devices to Process Buyer Data and shall promptly notify Buyer and Supplier of any lost, stolen, or otherwise compromised device that was used to Process Buyer Data in the manner required for the Breach Notifications pursuant to Section 4 of these Requirements.

3.7 Processing Changes. Supplier shall obtain Buyer's prior written consent before implementing any change to the Processing of Buyer Data. Supplier shall use commercially reasonable efforts to provide Buyer at least ninety (90) days' notice in advance of the proposed effective date of such change. To the extent Supplier implements any such change that results in a material reduction in Supplier's Security without Buyer's written consent, Buyer shall have the right to terminate the Agreement or the applicable SOW effective immediately upon written notice to Supplier.

3.8 Qualified Security Coordinator. Supplier shall assign an appropriate qualified security professional working for Supplier that shall act as its Security Coordinator, who will be the security liaison between Buyer and Supplier.

3.9 Additional Security Required. During the term of the Agreement, Supplier shall implement and maintain additional Security, as mutually agreed upon by Supplier and Buyer, in the event of: (a) any material changes to Services; (b) any Security Breach or Security Incident; or (c) any material decreases to Supplier's Security; provided, that the failure of Buyer to make a request of Supplier shall not impact, eliminate, or decrease Supplier's obligations under these Requirements.

3.10 Assistance for Buyer's Compliance. Supplier shall cooperate with Buyer's reasonable requests to assist Buyer with its own compliance objectives pursuant to Privacy and Security Laws, including, without limitation, completing any documentation, assessments, or questionnaires provided to Supplier regarding the same with complete and accurate information and complying with any data subjects' requests to block, correct, or delete their data from Supplier's systems consistent with Section 2.6 of these Requirements.

3.11 Regulator Requests. Supplier shall, to the extent permitted by law, notify Buyer immediately upon receipt of any request from a regulator to access Buyer Data, including any request to access any physical or virtual locations where such information is stored.

3.12 Identifying Violations. Supplier shall immediately notify Buyer if Supplier knows or reasonably believes that any written instruction given by Buyer would cause either party to violate applicable Privacy and Security laws. In the event of any conflict among any of Supplier's obligations as required herein, Supplier shall comply with the obligation that provides the most protective Security.

3.13 Conflicting Obligations. In the event of any conflict among any of Supplier's obligations as required herein or as required in the Agreement, Supplier shall comply with the obligation that provides the most protective Security.

3.14 Informing Personnel. Each of Supplier's employees, consultants, contractors, partners or agents who have been or will be involved in the provision of Services under the Agreement shall at all times be subject to professional, ethical, or contractual obligations of confidentiality with respect to Buyer Data that are no less restrictive than those applicable to Supplier under the Agreement.

3.15 Return of Buyer Data. Upon completion of contractual requirements or termination of the Agreement, Supplier shall return to Buyer all the information, data, documents and storage media which it has received and any copies thereof, including, but not limited to Buyer Data, in a commercially standard format reasonably accessible to Buyer, including any passwords, encryption keys, or other credentials necessary to access the same. Supplier shall provide evidence and confirm in writing that all the information, data, documents and storage media and any copies thereof, including, but not limited to Buyer Data, have been returned, and once Buyer has confirmed it has successfully accessed such information, deleted using methods reasonably contemplated to prevent the recovery or recreation of the data. Buyer may decide on an earlier date for data deletion at any time.

3.16 Security Coordinator**.** The Supplier shall ensure that its Security Coordinator is sufficiently trained, qualified and experienced to be able to fulfill the functions set out in these Requirements and any other functions that might reasonably be expected to be carried out by the individual as the Security Coordinator.

3.17 Additional Controls**.** During the Term of the Agreement, Supplier shall implement and maintain additional Security, as mutually agreed upon by Supplier and Buyer, in the event of: (i) any material changes to Services; (ii) any Security Breach; or (iii) any material decreases to Supplier's Security; provided, that the failure of Buyer to make a request of Supplier shall not impact, eliminate or decrease Supplier's obligations under these Requirements.

4. Security Breach Procedures.

4.1 Notice to Buyer. Supplier shall notify Buyer as soon as practicable, and in any event within 4 hours, after Supplier becomes aware of any Security Incident or Security Breach..

4.2 Contain and Remedy. Supplier shall, at its sole cost and expense, use best efforts to immediately remedy any Security Incident or Security Breach and prevent any further Security Incident or Security Breach at Supplier's expense in accordance with applicable privacy rights, laws, regulations and standards.

4.3 Investigate and Preserve. Supplier shall, at its sole cost and expense: (a) promptly preserve all relevant records, logs, files, data reporting, and other materials relevant to any Security Incident or Security Breach, and shall provide the same to Buyer upon request; and (b) diligently investigate any Security Incident or Security Breach and shall fully cooperate with Buyer in its own investigation of and response to any such Security Incident or Security Breach.

4.4 Cooperate with Buyer's Investigation. Supplier agrees to fully cooperate with Buyer in Buyer's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing Buyer with physical access to the facilities and operations affected; (iii) facilitating interviews with Supplier's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise required by Buyer.

4.5 Reimburse Costs. Supplier shall reimburse Buyer for all reasonable costs incurred by Buyer in responding to, and mitigating damages caused by, any such Security Incident or Security Breach, including, without limitation, all costs of notice and credit monitoring and identity theft protection services.

4.6 Buyer Controls Notices. Unless otherwise required by law, Supplier agrees that it shall not inform any third party of any Security Incident or Security Breach without first obtaining Buyer's prior written consent, other than to inform a complainant that the matter has been forwarded to Buyer's legal counsel. Supplier agrees not to include Buyer's name, logo, or any other identifiable information about Buyer or its affiliates in any notice or public statement concerning any Security Incident or Security Breach without Buyer's prior written approval. Further, Supplier agrees that Buyer shall have the sole right to determine: (i) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Buyer's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

5. Subcontractors.

5.1 Access for Subcontractor. Supplier shall not provide any subcontractor with direct or indirect access to Buyer Data, unless (i) it has received prior written consent from Buyer or (ii) such access is specifically allowed under the Agreement or applicable mutually signed SOW. Except as allowed per the foregoing sentence, Supplier shall not provide any third party (other than Supplier's regulators) with access to Supplier's systems or network that would allow the third party to have access to Buyer Data.

5.2 Investigation of Subcontractors. Notwithstanding Buyer's prior written consent, prior to providing any subcontractor with direct or indirect access to Buyer's Data or to Supplier's systems or network that would allow subcontractor access to Buyer Data, Supplier shall: (a) conduct a reasonable investigation of such subcontractor's information security measures, data protection procedures, and incident response measures to determine that such security is reasonable and consistent with Supplier's obligations under these Requirements; and (b) ensure that such subcontractor is obligated by law or contract to protect Buyer Data and cooperate with Buyer in the event of an incident or Security Breach consistent with these Requirements, in the same manner as required of Supplier. In all events, Supplier is and shall remain fully responsible for any act, error or omission of any subcontractor to whom Supplier grants access to Buyer Data or to Supplier's systems or network that would allow access to Buyer Data with respect to compliance with these Requirements, as if such act, error, or omission was undertaken by Supplier.

5.3 Only As Needed. Once the requirements of Sections 5.1 and 5.2 are met, Supplier shall only provide access to Buyer Data or to Supplier's systems that would allow subcontractors access to Buyer Data to the extent necessary for Supplier to perform the Services for Buyer. Once any such subcontractor no longer needs access to Buyer Data in order for Supplier to perform Services for Buyer, Supplier shall immediately terminate such subcontractor's access to such Buyer Data, or, if applicable, shall immediately request that Buyer terminate such access.

6. Audits and Monitoring.

6.1 Monitoring Access to Buyer Systems. Supplier agrees to allow Buyer and its representatives to, and Supplier shall secure Buyer and its representatives' rights to, monitor, log, and analyze the access of Supplier and each of its subcontractors within Buyer Systems as a condition of allowing such access.

6.2 Right to Audit. Upon Buyer's written request, and no less than annually, Supplier must permit Buyer or its representative to audit any and each of Supplier's privacy and security controls in relation to any Buyer Data being Processed by Supplier. Supplier shall fully cooperate with such audit by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software relevant to Supplier's compliance with these Requirements. Supplier shall make available documentation from its subcontractors to support Buyer's audit upon Buyer's request.

6.3 External Assessment and Certification. Supplier shall, at its sole cost and expense, maintain sufficient and current external security assessments of controls relevant to the Processing of Buyer Data to demonstrate Supplier's compliance with these Requirements ("**Assessments**") and provide a copy of such Assessments to Buyer upon request. Sufficient Assessments include a SOC-2 Type 2 report, ISO 27001 certification, CSA Security Trust Assurance and Risk (STAR) Level 2 certification, or other external audit or report that may be agreed upon by Buyer. Supplier will notify Buyer immediately if Supplier fails an Assessment. Supplier shall make available documentation to support Supplier's external audits upon Buyer's request.

6.4 Available Reports. Without limiting the foregoing, Supplier must, at the Supplier's expense, make available to Buyer a copy of Supplier's most recent SOC-2 Type 2 Report on Controls Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy.

6.5 Buyer's Right to Require Compliance. Following any audit by Buyer or Buyer's review of Supplier's most recent Assessments, Buyer may elect to recommend or require reasonable changes that Supplier must implement within a reasonable time frame. Supplier shall, as soon as reasonably practicable and at its sole cost and expense, implement any such measures requested in writing by Buyer which are reasonably necessary for Supplier to meet its obligations under these Requirements.

7. Breach of Requirements.

A Security Breach arising, in whole or in part, from an act or omission of Supplier or breach of Supplier's obligations under these Requirements shall constitute an event of default under the Agreement entitling Buyer to terminate the Agreement or the applicable SOW immediately and without opportunity to cure by providing written notice of such termination to Supplier. Without limitation to any other right or remedy set forth in these Requirements, the Agreement, or the applicable SOW, in the event that the Agreement or any SOW thereunder is terminated by Supplier pursuant to this Section 8.4, Buyer shall be entitled to recover from Supplier the reasonable costs incurred by Buyer in obtaining services from an alternate vendor to replace the terminated Services. Additionally, if Buyer so elects in its sole discretion, Supplier shall, upon written notice from Buyer, continue to provide the terminated Services in accordance with the Agreement and the applicable SOW until such time as Buyer can obtain such replacement services from an alternate vendor, provided that: (a) Supplier shall be entitled to standard compensation as set forth in the applicable SOW for its performance of the terminated Services during such period; and (b) in no event shall Supplier have any obligation under this provision to provide the terminated Services past the date that the term of the applicable SOW would have otherwise expired.

8. Representations and Warranties. Supplier represents and warrants that:

8.1 It routinely uses industry standard processes to check its systems and software ("**IT Service**") for malicious code, including, without limitation, viruses, Trojan horses, worms, and any other software routines or code designed to (i) permit unauthorized access by third parties, or (ii) disable, erase, or otherwise harm the IT Service, data, other software or hardware (collectively, "**Malicious Code**") and that the IT Service, when accessed by Buyer or users, will contain no Malicious Code.

8.2 It routinely, but no less than once a year, has a third party conduct penetration testing and perform vulnerability scans.

8.3 Each of Supplier's employees, consultants, contractors, partners or agents who have been or will be involved in the provision of Services under the Agreement have signed or will sign an agreement with Supplier agreeing not to use or disclose any Buyer Data other than as required for Supplier's performance of its obligations under this Agreement

8.4 Its collection, access, use, storage, disposal and disclosure of Buyer Data does and will comply with all applicable federal and, state, and foreign laws, as well as all other applicable regulations and directives, including, but not limited to Privacy and Security Laws.

8.5 It has conducted a criminal background investigation on each employee who will be involved in the provision of Services under the Agreement and further warrants that each of said employees has not been convicted of any felony or a misdemeanor involving crimes of violence, fraud, misappropriation, or other breach of trust.

9. Insurance Coverage.

In addition to any insurance requirements specified in the Agreement or any Exhibits thereto, Supplier shall also maintain Privacy and Network Security (otherwise known as Cyber Liability) coverage which includes providing protection against liability for (a) system attacks, (b) denial or loss of service attacks, (c) spread of malicious software code, (d) unauthorized access and use of computer systems, (e) social engineering attacks, (f) crisis management and customer notification expenses, (g) privacy regulatory defense and penalty reimbursement costs and (h) liability arising from the loss or disclosure of data that includes any Buyer Data, in each case with coverage limits of not less than $5,000,000 per occurrence. Prior to commencing any performance under the Agreement, Supplier shall provide Buyer with a certificate of insurance evidencing the insurance coverage required in this Section 9, in addition to any insurance specified in the Agreement or any Exhibits thereto.

10. Term and Termination.

10.1 Term. These Requirements shall be effective as of the Effective Date of the Agreement, and shall remain in effect until the later of either: (a) the duration of the Agreement; or (b) for so long as Supplier or any of its subcontractors continues to Process Buyer Data, provided that Buyer may reasonably assume that Supplier's and its subcontractors' Processing activities are continuing until Buyer receives written confirmation from Supplier to the contrary.

10.2 Termination by Buyer. These Requirements may be terminated by Buyer for any reason upon thirty (30) days' written notice to Supplier.

10.3 Buyer Data on Termination or Expiration. Promptly upon expiration or termination of the Agreement or anytime earlier upon Buyer's prior written request, Supplier shall, at its sole cost and expense, permanently delete or migrate to Buyer or any third-party vendor of Buyer (the choice to be made by Buyer in its sole discretion), and shall cause its subcontractors to do the same, any and all Buyer Data in Supplier's or its subcontractors' possession or control, including, without limitation, from backup and archival sources, in compliance with industry standards, Privacy and Security Laws, and otherwise as specified in these Requirements. To the extent Buyer Data is to be permanently deleted under this provision, Supplier will not undertake such permanent deletion without confirming such instructions with Buyer and then Supplier will, upon Buyer's request, provide written certification of the permanent deletion of such Buyer Data. To the extent Buyer Data is to be migrated to Buyer or another third-party vendor under this provision, such Buyer Data will be in a format specified by Buyer or, if not specified, in a platform-agnostic format, and Supplier shall, at its sole cost and expense, reasonably cooperate with Buyer and the recipient third-party vendor (if applicable) as necessary to carry out such migration.

11. Miscellaneous.

11.1 Equitable Relief. Supplier recognizes that serious and irreparable injury could result to Buyer if Supplier breaches its obligations under these Requirements. Therefore, Supplier agrees that Buyer will be entitled to seek a restraining order, injunction, or other equitable relief without the need to post bond if Supplier breaches its obligations under these Requirements, in addition to any other remedies and damages that would be available at law or in equity.

11.2 Indemnification. Without limitation to any other indemnification obligation under the Agreement, Supplier shall defend, indemnify, and hold harmless Buyer, its affiliates, and each of their respective employees, officers, directors, agents, and representatives from and against all liabilities, losses, damages, judgments, settlements, obligations, fines, costs, and expenses of any nature (including, without limitation,

reasonable attorneys' fees and litigation costs) incurred in connection with any claim, action, cause of action, suit, demand, or proceeding threatened or asserted by any third party (including, without limitation, any government entity) arising out of, relating to, or resulting from (i) any Security Incident or Security Breach arising, in whole or in part, from an act or omission of Supplier or (ii) any failure by Supplier to comply with any of the requirements set forth in these Requirements.

11.3 Liability. BUYER'S DAMAGES RESULTING FROM (I) ANY SECURITY INCIDENT OR SECURITY BREACH ARISING, IN WHOLE OR IN PART, FROM AN ACT OR OMISSION OF SUPPLIER OR (II) ANY FAILURE BY SUPPLIER TO COMPLY WITH ANY OF THE OBLIGATIONS SET FORTH IN THESE REQUIREMENTS ARE NOT SUBJECT TO ANY LIMITATIONS OR EXCLUSIONS OF LIABILITY SET FORTH IN THE AGREEMENT. FURTHER, THE FOLLOWING REASONABLE COSTS SHALL BE CONSIDERED DIRECT DAMAGES IF SUSTAINED BY BUYER ARISING OUT OF ANY SUCH SECURITY INCIDENT OR SECURITY BREACH OR ANY FAILURE BY SUPPLIER TO COMPLY WITH ANY OF THE OBLIGATIONS SET FORTH IN THESE REQUIREMENTS: (A) COSTS ARISING FROM PROCURING SERVICES FROM AN ALTERNATIVE SOURCE; (B) COSTS ARISING FROM RECREATING OR RELOADING LOST OR DAMAGED BUYER DATA; (C) COSTS ARISING FROM BUYER'S INVESTIGATION OR REMEDIATION OF SUCH SECURITY INCIDENT OR SECURITY BREACH OR FAILURE OF SUPPLIER TO COMPLY WITH THE OBLIGATIONS SET FORTH IN THESE REQUIREMENTS, INCLUDING, WITHOUT LIMITATION, FORENSIC INVESTIGATION, PREPARATION AND DELIVERY OF NOTIFICATION, PREPARATION AND DELIVERY OF CALL CENTER SERVICES AND PROVISION OF CREDIT MONITORING AND IDENTITY THEFT PROTECTION SERVICES; AND (D) LEGAL FEES ASSOCIATED WITH EACH OF THE FOREGOING.

12. State-Specific Provisions.

12.1 California Consumer Privacy Act Provisions.

12.1.1 Scope. The provisions of this Section 12.1 are included in these Requirements for the purpose of ensuring compliance with the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 *et seq.* (the "CCPA"). Except as modified in this Section 12.1, all other provisions of these Requirements shall remain in full force and effect.

12.1.2 Definitions. For purposes of this Section 12.1 only, the following terms shall have the following meanings: (i) "Buyer Personal Information" means any personal information that Buyer discloses to Supplier for any business purpose pursuant to the Agreement; (ii) "personal information" has the meaning set forth in Cal. Civ. Code § 1798.140(o); (iii) "business purpose" has the meaning set forth in Cal. Civ. Code § 1798.140(d); (iv) "commercial purpose" has the meaning set forth in Cal. Civ. Code § 1798.140(f); (v) "sell" has the meaning set forth in Cal. Civ. Code § 1798.140(t); and (vi) "service" has the meaning set forth in Cal. Civ. Code § 1798.140(u).

12.1.3 Restrictions on Buyer Personal Information. Supplier is prohibited from: (i) selling any Buyer Personal Information; (ii) retaining, using, or disclosing any Buyer Personal Information for any purpose other than for the specific purpose of performing the Services, including retaining, using, or disclosing the Buyer Personal Information for any commercial purpose other than providing the Services; and (iii) retaining, using, or disclosing any Buyer Personal Information outside of the direct business relationship between Buyer and Supplier.

12.1.4 Certification. By signing the Agreement, Supplier certifies that it understands the restrictions in Section 12.1(c) and will comply with them.